DECLARATION OF HIDEMA TANAKA, TOSHINOBU KANEKO, AND NOBUYUKI SUGIO

1. We, Hidema Tanaka, residing in Koganei, Japan, Toshinobu Kaneko, residing in Noda, Japan, and Nobuyuki Sugio, residing in Noda, Japan, declare:

2. We are employed by Communications Research Laboratory, Independent Administrative Institution, 4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo, Japan.

3. We are the inventors of the claimed subject matter in the current application, U.S. Patent Application Serial No. 10/762,654 filed on January 21, 2004.

4. We signed a Declaration on November 19, 2003, after reviewing an English language patent application including the specification, claims, and drawings which was subsequently filed as U.S. Patent Application Serial No. 10/762,654 in the United States of America.

5. The original Claim 9 as filed and currently at issue is disclosed in the specification filed as U.S. Patent Application Serial No. 10/762,654 in the United States of America.

6. The preamble of the original Claim 9 as filed, "A weak key detector used along with an encryption apparatus having a key schedule part for calculating an extended key from a user key for detecting a weak key that is one kind of a user key to lower difficulty in decrypting ciphertext obtained by the encryption apparatus, the weak key detector" is disclosed on pages 17-19 of the specification.

7. The first element of the original Claim 9 as filed, "a weak key information storing part for storing segment bit patterns of the user key and the extended key forming a weak key condition satisfied by the weak key as weak key information" is disclosed on pages 18-19 of the specification and Figure 12 as reference numeral 6.

8. The portion of the first element of the original Claim 9 as filed, "segment bit patterns of the user key and the extended key forming a weak key condition satisfied by the weak key as weak key information" is disclosed on pages 12-13 of the specification.

9. The second element of the original Claim 9 as filed "a determining part for accepting a user key to determine whether the user key is a weak key based on the weak key information" is disclosed on pages 18-19 of the specification and Figure 12 as reference numeral 5.

10. The third element of the original Claim 9 as filed, "wherein the determining part includes . . . a key schedule part for calculating the extended key from the user key, as similar to that provided for the encryption apparatus" in Claim 9 is disclosed on pages 18-19 of the specification and Figure 12 as reference numeral 51.

11. The fourth element of the original Claim 9 as filed, "wherein the determining part includes . . . a determining part main body for determining whether the user key and the extended key satisfy the weak key condition to output a detection signal indicating a result" in Claim 9 is disclosed on pages 18-19 of the specification and Figure 12 as reference numeral 52.

12. The portion of the fourth element of the original Claim 9 as filed, "whether the user key and the extended key satisfy the weak key condition" is disclosed on pages 12-13 of the specification.

13. We also gave a presentation on the subject matter which forms the basis of the original Claim 9 as filed on January 27, 2003 at the 2003 Symposium on Cryptography and Information Security in Hamamatsu, Japan.

14. The presentation was published as an article on January 26, 2003 with an English translated title "A study on attack considering key schedule against block ciphers" in Volume 1 of Proceedings of the 2003 Symposium on Cryptography and Information Security on pages 363-68.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Executed this 5th day of September, 2007, at Tokyo, Japan

Hidema Tanaka

Hidema Tanaka

Executed this 15th day of September, 2007, at Noda, Japan

Toshinobu Kaneko

Toshinobu Kaneko

Executed this 5th day of September, 2007, at Noda, Japan

Nobuyuki Sugio

Nobuyuki Sugio